Manuel d'utilisation du client VPN

9235967
Édition 1

Copyright © 2004 Nokia. Tous droits réservés.
La reproduction, le transfert, la distribution ou le stockage d'une partie ou de la totalité du contenu de ce document, sous quelque forme que ce soit, sans l'autorisation écrite préalable de Nokia est interdite.
Nokia est une marque déposée de Nokia Corporation. Les autres noms de produits et de sociétés mentionnés dans ce document peuvent être des marques commerciales ou des noms de marques de leurs détenteurs respectifs.
Symbian et Symbian OS sont des marques commerciales de Symbian Ltd.
SecurID est une marque déposée de RSA Security INC.
Nokia applique une méthode de développement continu. Par conséquent, Nokia se réserve le droit d'apporter des changements et des améliorations à tout produit décrit dans ce document, sans aucun préavis.
Nokia ne peut en aucun cas être tenue pour responsable de toute perte de données ou de revenu, ainsi que de tout dommage particulier, incident, consécutif ou indirect.
Le contenu de ce document est fourni "en l'état". À l'exception des lois obligatoires applicables, aucune garantie sous quelque forme que ce soit, explicite ou implicite, y compris, mais sans s'y limiter, les garanties implicites d'aptitude à la commercialisation et d'adéquation à un usage particulier, n'est accordée quant à la précision, à la fiabilité ou au contenu du document. Nokia se réserve le droit de réviser ce document ou de le retirer à n'importe quel moment sans préavis.
Pour vous assurer de la disponibilité des produits, qui peut varier en fonction des régions, contactez votre revendeur Nokia le plus proche.

Table des matières

Réseau privé virtuel 4

Installation 6

Configuration système requise 6

Politiques VPN 7

Installer des politiques VPN depuis des serveurs de politiques VPN 7
Installer des politiques VPN depuis des fichiers SIS 8
Visualiser les politiques VPN 9
État de la politique 10
État du certificat 10
Créer des points d'accès VPN avec les valeurs par défaut 11
Mettre à jour les politiques VPN 11
Supprimer des politiques VPN 12

Serveurs de politiques VPN 13

Se connecter aux serveurs de politiques VPN 13
Installer les paramètres depuis des fichiers SIS 13
Visualiser les serveurs de politiques VPN 14
Ajouter des serveurs de politiques VPN 14
Modifier les serveurs de politiques VPN 16
Synchroniser les serveurs de politiques VPN 16
Enregistrer des certificats VPN 17
Supprimer des serveurs de politiques VPN 17

Points d'accès VPN 18

Visualiser les points d'accès VPN 18
Créer des points d'accès VPN 18
Supprimer des points d'accès VPN 19

Journal VPN 20

Visualiser le journal VPN 20
Effacer le journal VPN 20

Mots de passe d'enregistrement de clé . 21

Créer ou modifier un mot de passe d'enregistrement de clé 21
Saisir des mots de passe d'enregistrement de clé 22

VPN et applications 23

S'authentifier sur les passerelles VPN 23

Dépannage 25

1. Réseau privé virtuel

Allez à *Menu* et sélectionnez *Outils* > *Paramètres* > *Paramètres de connexion* > *Réseau privé virtuel (VPN)*.

Un **réseau privé virtuel** (VPN, Virtual Private Network) vous permet de créer des connexions cryptées vers les informations dont vous avez besoin lorsque vous êtes en déplacement. Ainsi, vous pouvez accéder de façon sécurisée à votre réseau d'entreprise pour garder le contact et effectuer des traitements dans votre courrier électronique, dans les applications de base de données et sur l'intranet.

Pour créer un VPN, une passerelle et l'appareil mobile s'authentifient mutuellement et négocient les algorithmes de cryptage et d'authentification qui préserveront la confidentialité et l'intégrité des informations auxquelles vous accéderez.

Pour créer des connexions VPN, vous devez d'abord créer des points d'accès VPN, puis sélectionner ceux–ci lorsque vous vous connectez à votre réseau d'entreprise avec des applications. Une connexion VPN au réseau d'entreprise est créée via un autre type de connexion Internet. Celle–ci est créée et les données sont cryptées conformément à une politique VPN dont les paramètres sont chargés lorsque vous vous connectez à un point d'accès VPN.

Remarque : Pour que vous puissiez utiliser le VPN, les administrateurs doivent vous fournir les paramètres du serveur de politiques VPN. Ils peuvent vous les envoyer sous forme de fichier SIS, **Symbian Installation System**.

Pour utiliser un VPN

1 Installez le VPN Client.
Pour plus d'informations, consultez la section "Installation", page 6.

2 Configurez une connexion à un serveur de politiques VPN.
Vous pouvez configurer les paramètres d'un serveur de politiques VPN ou bien installer ces paramètres depuis un fichier SIS.
Pour plus d'informations, consultez la section "Se connecter aux serveurs de politiques VPN", page 12.

Remarque : Si vous installez les politiques VPN depuis des fichiers SIS, il est inutile de créer des connexions vers des serveurs de politiques VPN.

3 Installez les politiques VPN depuis le serveur de politiques VPN.
Pour plus d'informations, consultez la section "Installer des politiques VPN depuis des serveurs de politiques VPN", page 7.

4 Créez des points d'accès VPN.
Chacun de ces points spécifie un point d'accès Internet et une politique VPN.
Pour plus d'informations, consultez la section "Créer des points d'accès VPN", page 17.

Remarque : Les points d'accès VPN associent des politiques à des points d'accès Internet. Lorsque vous synchronisez un serveur de politiques VPN pour la première fois, un point d'accès VPN est créé pour chacune des politiques que vous installez sur l'appareil mobile.

5 Sélectionnez un point d'accès VPN si vous utilisez des applications pour vous connecter au réseau de l'entreprise.
Pour plus d'informations, consultez la section "VPN et applications", page 21.
Une connexion VPN est créée "au-dessus" de la connexion Internet.

2. Installation

Vous recevez VPN client sous forme de fichier SIS (**Symbian installation system**) standard.

Pour installer VPN client sur un appareil mobile compatible, vous devez procéder comme avec tout autre logiciel. Pour plus d'informations sur l'installation de logiciels sur l'appareil mobile, consultez la documentation relative à celui–ci.

Lorsque l'installation est terminée, éteignez puis rallumez l'appareil mobile pour que les modifications prennent effet.

Il est inutile de conserver le fichier SIS de VPN client après l'installation. Supprimez–le pour libérer de la mémoire.

Configuration système requise

Pendant l'installation de VPN client, l'appareil mobile doit disposer d'au moins 1,5 Mo de mémoire libre.

Après l'installation, VPN client réserve 900 Ko de mémoire sur l'appareil mobile ou sur une carte mémoire. En général, chaque politique VPN requiert de 1 à 16 Ko de mémoire sur l'appareil mobile.

3. Politiques VPN

Les **politiques VPN** déterminent la méthode utilisée par un appareil mobile et une passerelle VPN pour s'authentifier mutuellement, ainsi que les algorithmes servant à crypter les données. Ce sont les administrateurs qui créent les politiques VPN. Ensuite, ils les enregistrent sur des serveurs de politiques VPN ou les fournissent sous forme de fichiers SIS (**Symbian Installation System**). Vous pouvez installer des politiques VPN depuis un serveur ou depuis des fichiers SIS.

Allez à *Menu* et sélectionnez *Outils* > *Paramètres* > *Paramètres de connexion* > *Réseau privé virtuel (VPN)* > *Gestion VPN* > *Politiques VPN*.

Installer des politiques VPN depuis des serveurs de politiques VPN

Pour installer des politiques VPN

1 Appuyez sur *Oui* lorsque vous ouvrez un écran *Politiques VPN* vide et que vous êtes invité à installer des politiques VPN.
2 Appuyez sur *Oui* lorsque vous êtes invité à ajouter des serveurs de politiques VPN.
3 Configurez les paramètres de connexion à un serveur de politiques VPN.
Pour plus d'informations, consultez la section "Se connecter aux serveurs de politiques VPN", page 12.
4 Appuyez sur *Oui* lorsque vous êtes invité à synchroniser le serveur de politiques VPN.
5 Créez un **mot de passe d'enregistrement de clé**.

Glossaire : Les serveurs de politiques VPN sont des serveurs faisant partie du réseau de l'entreprise et contenant des politiques VPN.

Glossaire : Le mot de passe d'enregistrement de clé permet de protéger les clés privées des politiques VPN et les connexions au serveur de politiques VPN contre toute utilisation non autorisée.

Glossaire : Le code d'identification du serveur de politiques VPN peut être considéré comme "l'empreinte digitale" du certificat de ce serveur.

Glossaire : Le mot de passe d'importation de clé permet de protéger les clés privées stockées dans un fichier de politiques VPN.

Pour plus d'informations, consultez la section "Créer ou modifier un mot de passe d'enregistrement de clé", page 20.
Connectez–vous au serveur de politiques VPN.

6 Vérifiez le **code d'identification du serveur de politiques VPN** afin d'établir une relation sécurisée.
Vous pouvez ignorer cette étape si vous configurez les paramètres du serveur de politiques VPN depuis un fichier SIS.
Pour plus d'informations, consultez la section "Ajouter des serveurs de politiques VPN", page 13.

7 Saisissez les informations d'authentification requises pour accéder au serveur de politiques VPN et appuyez sur *OK*.
L'administrateur du serveur de politiques VPN doit vous fournir ces informations.

8 Les politiques VPN sont installées sur l'appareil mobile.

9Remarque : Si vous appuyez sur *Quitter*, les politiques VPN ne sont pas installées. Appuyez sur *Options* et sélectionnez *Installer politique* pour installer des politiques VPN depuis un serveur de politiques VPN.

Installer des politiques VPN depuis des fichiers SIS

Les administrateurs peuvent vous fournir les politiques VPN sous forme de fichiers SIS. Si vous installez des politiques VPN depuis des fichiers SIS, il est inutile de définir des connexions vers des serveurs de politiques VPN. Après avoir installé les politiques, vous pouvez créer des points d'accès VPN et les associer à des applications.

Si les politiques contiennent des clés privées et les certificats correspondants, les administrateurs peuvent définir des **mots de passe d'importation de clé** afin de protéger les clés privées. Il est recommandé aux administrateurs d'utiliser une méthode sécurisée pour vous faire parvenir un tel mot de passe.

Pour installer des politiques VPN depuis des fichiers SIS

1 Saisissez le mot de passe d'importation de clé dans *Mot de passe importation de clé:* et appuyez sur *OK*.
2 Saisissez le mot de passe d'enregistrement de clé dans *Mot de passe enregistrement de clé:* et appuyez sur *OK*.

Visualiser les politiques VPN

L'écran *Politiques VPN* répertorie les politiques VPN que vous avez installées sur l'appareil mobile.

Si *(aucune politique VPN)* est affiché, vous devez installer des politiques VPN. Appuyez sur *Options* et sélectionnez *Installer politique* pour installer des politiques VPN depuis un serveur de politiques VPN.

Sélectionnez une politique VPN pour afficher les informations suivantes :

- *Description:* : affiche des informations complémentaires sur la politique. La description est saisie par l'administrateur lors de la création de la politique.
- *Etat de la politique:* : indique si la politique VPN est prête à être utilisée ou si elle est déjà en cours d'utilisation.
- *Etat du certificat:* : indique si des certificats utilisateur valides sont disponibles sur l'appareil mobile.
- *Nom de la politique:* : nom que les administrateurs ont donné à la politique VPN lors de sa création.
- *Serveur de politiques:* : indique le nom du serveur de politiques VPN à partir duquel vous avez installé la règle. Ce nom a été défini lors de la configuration des connexions vers les serveurs de politiques VPN. Ce champ est masqué si vous avez installé la politique depuis un fichier SIS.
- *Mis à jour:* : affiche la date de la dernière mise à jour de la politique depuis le serveur. Ce champ est masqué si vous avez installé la politique depuis un fichier SIS.

État de la politique

Remarque : L'écran affichant les informations sur la politique n'est pas réactualisé si l'état de celle–ci change tandis que cet écran est ouvert.

Etat de la politique: peut prendre les valeurs suivantes :

- *Utilisé* : vous avez créé une connexion avec un point d'accès VPN associé à la politique VPN. La politique entre en service lorsque vous créez une connexion.
- *Associé à un point d'accès VPN* : vous avez associé la politique à un ou plusieurs points d'accès VPN. Vous pouvez sélectionner le point d'accès VPN de votre choix pour mettre en service la politique.
- *Non associé à un point d'accès VPN* : vous devez associer la politique à un point d'accès VPN pour que cette politique entre en service.

État du certificat

Etat du certificat: peut prendre les valeurs suivantes :

- *OK* : au moins un certificat valide est disponible dans l'appareil mobile ou vous n'utilisez pas de certificat pour vous authentifier sur les passerelles VPN.
- *Expiré* : la durée de validité d'un ou de plusieurs certificats a expiré.
  Si vous ne parvenez pas à créer de connexion VPN, essayez de mettre à jour la politique VPN afin d'enregistrer de nouveaux certificats.
- *Aucun certificat* : un ou plusieurs des certificats requis sont introuvables sur l'appareil mobile.
  Si vous ne parvenez pas à créer de connexion VPN, essayez de mettre à jour la politique VPN afin d'enregistrer de nouveaux certificats.
- *Pas encore valide* : un ou plusieurs certificats sont destinés à une utilisation ultérieure. Cette valeur peut également signifier que la date et l'heure de l'appareil mobile sont définies dans le passé, que les fuseaux horaires sont incorrectement configurés ou que le paramètre d'horaire été/hiver est activé.

Appuyez sur la touche écran pour fermer l'affichage des informations et revenir à l'écran *Politiques VPN*.

Créer des points d'accès VPN avec les valeurs par défaut

Pour pouvoir utiliser la politique VPN, vous devez l'associer à un point d'accès VPN. Appuyez sur *Options* et sélectionnez *Définir pt accès VPN* dans l'écran *Politiques VPN*.

Le client VPN mobile crée un point d'accès VPN avec des paramètres par défaut. Vous pouvez créer et modifier les points d'accès VPN dans l'écran des points d'accès VPN.

Cette option n'est pas disponible si vous avez installé la politique depuis un fichier SIS.

Mettre à jour les politiques VPN

Lorsque vous créez une connexion vers un point d'accès VPN, l'état de la politique VPN est vérifié sur le serveur de politiques VPN. Si les administrateurs ont créé une nouvelle version de la politique, celle–ci est installée sur l'appareil mobile. S'ils ont supprimé la politique du serveur, elle est supprimée de l'appareil mobile.

Les modifications prendront effet la prochaine fois que vous établirez une connexion vers le point d'accès VPN. Elles n'affectent pas la connexion actuelle.

Vous pouvez également mettre à jour une politique VPN dans l'écran *Politiques VPN*. Pour mettre à jour une politique VPN, sélectionnez celle–ci puis appuyez sur *Options* et sélectionnez *Mise à jr politique*. L'état de la politique VPN est vérifié sur le serveur de politiques VPN.

Supprimer des politiques VPN

Les politiques VPN sont supprimées automatiquement lorsque vous synchronisez un serveur de politiques VPN après que les administrateurs aient supprimé ces politiques sur ce serveur. Si vous supprimez une politique VPN qui existe encore sur le serveur, elle est réinstallée lorsque vous synchronisez des politiques depuis le serveur.

Pour supprimer une politique VPN, sélectionnez–la et appuyez sur la touche d'effacement.

Vous ne pouvez plus utiliser un point d'accès VPN si vous supprimez une politique qui lui est associée.

4. Serveurs de politiques VPN

Vous pouvez installer des politiques VPN depuis des serveurs de politiques VPN. Lorsque vous créez une connexion vers un point d'accès VPN, la politique VPN associée à ce point est automatiquement mise à jour depuis un serveur de politiques VPN. Pour mettre à jour toutes les politiques VPN, synchronisez les serveurs de politiques VPN avec l'appareil mobile. Pour plus d'informations, consultez la section "Synchroniser les serveurs de politiques VPN" on page 16.

Allez à *Menu* et sélectionnez *Outils* > *Paramètres* > *Paramètres de connexion* > *Réseau privé virtuel (VPN)* > *Gestion VPN* > *Serveurs de pol. VPN*.

Se connecter aux serveurs de politiques VPN

Lorsque vous installez des politiques VPN depuis un serveur de politiques VPN, vous établissez une relation sécurisée entre l'appareil mobile et le serveur. Pour cela, vous devez authentifier le serveur et vice versa.

Une fois que le serveur de politiques VPN vous a authentifié, une clé privée est générée et le certificat correspondant est enregistré. Le certificat vous authentifie sur le serveur. La clé privée et le certificat sont stockés dans un enregistrement de clé, sur l'appareil mobile.

Astuce : Les administrateurs peuvent vous fournir un fichier SIS contenant les paramètres permettant de se connecter à un serveur de politiques VPN, ou vous pouvez configurer vous-même ces paramètres.

Installer les paramètres depuis des fichiers SIS

Vous pouvez installer les paramètres du serveur de politiques VPN à partir d'un fichier SIS. La procédure d'installation des paramètres sur un appareil mobile est la même que pour tout autre logiciel.

Les paramètres se composent de l'adresse et du certificat du serveur. Grâce au certificat du serveur, l'appareil mobile considère le serveur de politiques VPN comme étant fiable. Il vous suffit donc de prouver votre identité en entrant votre nom d'utilisateur et votre mot de passe.

Le fichier SIS ne contient pas de paramètres permettant de se connecter au serveur de politiques VPN par le biais d'un point d'accès Internet. Pour configurer le point d'accès Internet, vous devez modifier les paramètres du serveur de politiques VPN. Vous pouvez également sélectionner le point d'accès Internet au moment où vous vous connectez au serveur de politiques VPN.

Si les administrateurs ne signent pas le fichier SIS, un avertissement de sécurité s'affiche lorsque vous installez le fichier SIS. Vous pouvez ignorer cet avertissement si vous êtes certain que l'administrateur du serveur de politiques VPN a créé le fichier SIS et que ce dernier n'a pas été modifié.

Quittez *Réseau privé virtuel (VPN)* avant de lancer l'installation des paramètres depuis un fichier SIS, faute de quoi l'installation échouera.

Visualiser les serveurs de politiques VPN

L'écran *Serveurs de politiques VPN* récapitule les serveurs de politiques VPN que vous avez créés.

Si *(aucun serveur de politiques VPN)* est affiché, vous devez créer des serveurs de politiques VPN. Pour ajouter un serveur de politiques VPN, appuyez sur *Options* et sélectionnez *Nouveau serveur*.

Ajouter des serveurs de politiques VPN

Si vous n'utilisez pas de fichier SIS pour installer les paramètres du serveur, vous devez configurer vous–même ces paramètres.

Lorsque vous vous connectez pour la première fois à l'adresse du serveur de politiques VPN, vous devez authentifier ce serveur. Les administrateurs vous fournissent le code d'identification du serveur. Vérifiez et complétez ce code.

Lorsque l'authentification a réussi, un certificat est enregistré à des fins d'authentification ultérieure sur le serveur.

Pour ajouter un serveur de politiques VPN

1 Appuyez sur *Options* et sélectionnez *Nouveau serveur* dans l'écran *Serveurs de politiques VPN*.

2 Sélectionnez *Nom du serv. de pol.* pour donner un nom au serveur et appuyez sur *OK*.
Vous pouvez saisir le nom de votre choix, à condition qu'il soit unique dans l'écran répertoriant les serveurs de politiques VPN.
Si vous laissez ce champ vide, la valeur de *Adresse serv. de pol.* y est insérée.
Le nom apparaît dans la liste des serveurs de politiques VPN et dans la barre de titre de la boîte de dialogue des paramètres du serveur.

3 Sélectionnez *Adresse serv. de pol.*, saisissez le nom d'hôte ou l'adresse IP du serveur à partir duquel seront installées les politiques VPN, puis appuyez sur *OK*.
Vous pouvez aussi indiquer un numéro de port (séparé par un signe deux points ":").
L'adresse du serveur est fournie par les administrateurs.

4 Sélectionnez *Pt d'accès à Internet*, associez le serveur à un point d'accès et appuyez sur *OK*.
Le point d'accès est utilisé pour la connexion à ce serveur.
Les administrateurs vous indiquent le point d'accès à sélectionner.

5 Appuyez sur *Retour* pour enregistrer les paramètres du serveur de politiques VPN.

6 Appuyez sur *Oui* lorsque vous êtes invité à **synchroniser** le serveur de politiques VPN.
Vous êtes invité à vérifier l'identité du serveur de politiques VPN.
Les administrateurs vous fournissent le code d'identification du serveur.

7 Comparez attentivement le code d'identification du serveur de politiques VPN affiché avec celui fourni par les administrateurs, saisissez les caractères manquants dans le champ et appuyez sur *OK*.

Glossaire : La synchronisation consiste à rechercher, sur un serveur de politiques VPN, les politiques qui ont été ajoutées, mises à jour ou supprimées.

Glossaire : Le nom d'utilisateur et le mot de passe protègent le serveur contre tout accès non autorisé.

8 Saisissez votre **nom d'utilisateur** dans *Nom d'utilisateur du serveur politiques:* et votre **mot de passe** dans *Mot de passe serveur de politiques:* pour vous authentifier auprès du serveur de politiques VPN et appuyez sur *OK*.
Les administrateurs vous indiquent le nom d'utilisateur et le mot de passe à saisir.

Un certificat est enregistré à des fins d'authentification ultérieure sur le serveur de politiques VPN et les politiques sont installées sur l'appareil mobile.

Vous pouvez ensuite créer des points d'accès VPN et les associer à des applications. Pour plus d'informations, consultez la section "Créer des points d'accès VPN", page 17.

Modifier les serveurs de politiques VPN

Sélectionnez un serveur dans l'écran *Serveurs de politiques VPN* afin d'afficher ou de modifier ses paramètres.

Sélectionnez *Nom du serv. de pol.* pour modifier son nom. L'écran *Serveurs de politiques VPN* affiche le nouveau nom.

Vous ne pouvez plus modifier le contenu du champ *Adresse serv. de pol.* après avoir installé des politiques VPN depuis le serveur, car ce dernier envoie cette adresse lors de la première connexion.

Si vous avez supprimé le point d'accès associé au serveur de politiques VPN, *Pt d'accès à Internet* affiche le texte (non sélectionné). Sélectionnez un point d'accès Internet afin de sélectionner un nouveau point d'accès. Si vous avez supprimé tous les points d'accès, vous ne pouvez pas enregistrer les paramètres.

Synchroniser les serveurs de politiques VPN

Sélectionnez un serveur de politiques VPN dans l'écran *Serveurs de politiques VPN*, appuyez sur *Options* et sélectionnez *Synchr. serveur* pour installer et mettre à jour des politiques depuis ce serveur. Les politiques qui ont été ajoutées, mises à jour ou supprimées sont recherchées sur le serveur.

Si le serveur comporte de nouvelles politiques ou versions de politiques VPN, celles–ci sont installées sur l'appareil mobile. Si les administrateurs ont supprimé des politiques du serveur, elles sont supprimées de l'appareil mobile.

Lorsque vous synchronisez un serveur de politiques VPN pour la première fois, un point d'accès VPN est créé pour chacune des politiques que vous installez sur l'appareil mobile. Vous pouvez créer et modifier les points d'accès VPN dans l'écran *Points d'accès VPN*.

Lorsque vous vous connectez à un serveur de politiques VPN pour installer ou mettre à jour des politiques, il se peut que vous deviez enregistrer des certificats VPN depuis le serveur.

Enregistrer des certificats VPN

Pour chacun des certificats requis, une demande de certification est créée et envoyée au serveur de politiques VPN. Le serveur enregistre chaque certificat demandé provenant d'une **autorité de certification** (CA, Certification Authority).

La demande de certification et le certificat correspondant contiennent votre identité utilisateur. Selon la configuration du serveur de politiques VPN, les certificats VPN peuvent utiliser le même identifiant utilisateur que le serveur. Si cela n'est pas possible, vous êtes invité à indiquer votre identifiant utilisateur pour un domaine spécifique.

Pour créer des demandes de certification

1 Saisissez votre identifiant utilisateur de certificat pour le domaine spécifique dans *Identité utilisateur pour :*.
Les administrateurs peuvent vous indiquer les informations à saisir.
2 Appuyez sur *OK*.

Supprimer des serveurs de politiques VPN

Pour supprimer un serveur de politiques VPN, sélectionnez–le dans l'écran *Serveurs de politiques VPN* et appuyez sur la touche d'effacement.

Confirmez la suppression des politiques VPN que vous avez installées depuis le serveur.

5. Points d'accès VPN

Allez à *Menu* et sélectionnez *Outils* > *Paramètres* > *Paramètres de connexion* > *Réseau privé virtuel (VPN)* > *Points d'accès VPN*.

Un point d'accès VPN est un point d'accès virtuel associant une politique VPN et un point d'accès Internet. Sélectionnez un point d'accès VPN dans les listes de points d'accès Internet pour créer une connexion VPN.

Visualiser les points d'accès VPN

L'écran *Points d'accès VPN* répertorie les points d'accès VPN que vous avez créés sur l'appareil mobile. Le texte *(aucun point d'accès VPN)* signifie que vous n'avez créé aucun point d'accès VPN. Pour en créer un, appuyez sur *Options* et sélectionnez *Nveau point d'accès*.

Sélectionnez un point d'accès VPN puis sélectionnez *Options* > *Modifier* pour afficher et modifier les informations suivantes :

- *Nom de la connexion* : identifie le point d'accès VPN dans les listes de points d'accès.
- *VPN policy* : nom de la politique VPN associée au point d'accès VPN.
- *Pt d'accès à Internet* : nom du point d'accès par lequel passe la connexion VPN créée.
- *Adresse serv. proxy* : adresse d'un serveur proxy faisant partie du réseau de l'entreprise.
- *N° port serv. proxy* : numéro de port utilisé pour la connexion au serveur proxy.

Créer des points d'accès VPN

La première fois que vous ouvrez l'écran *Points d'accès VPN*, vous êtes invité à créer des points d'accès VPN. Appuyez sur *Oui*.

Pour créer des points d'accès VPN

1 Appuyez sur *Options* et sélectionnez *New access point*.
2 Sélectionnez *Nom de la connexion* pour modifier le nom de la connexion. Vous pouvez entrer le nom de votre choix.
3 Sélectionnez *VPN policy* pour définir le mode de cryptage de la connexion. Si la liste est vide, vous devez installer des politiques VPN depuis des fichiers SIS ou depuis des serveurs de politiques VPN.
4 Sélectionnez *Pt d'accès à Internet* pour désigner le point d'accès devant être utilisé pour la connexion VPN. Si la liste est vide, vous devez créer des points d'accès.
5 Sélectionnez *Adresse serv. proxy* pour saisir l'adresse d'un serveur proxy faisant partie du réseau de l'entreprise.
6 Sélectionnez *N° port serv. proxy* pour modifier le port par défaut, 80.

Astuce : Si vous spécifiez un serveur proxy dans les paramètres de point d'accès VPN, vous n'avez pas à le spécifier dans les paramètres du navigateur Internet.

Supprimer des points d'accès VPN

Pour supprimer un point d'accès VPN, sélectionnez–le dans l'écran *Points d'accès VPN* puis appuyez sur la touche d'effacement.

6. Journal VPN

Allez à *Menu* et sélectionnez *Outils* > *Paramètres* > *Paramètres de connexion* > *Réseau privé virtuel (VPN)* > *Gestion VPN* > *Journal VPN*.

Icônes : indique une erreur, un avertissement et une description.

Ce journal contient des messages qui sont enregistrés lorsque vous mettez à jour et synchronisez des politiques VPN et créez des connexions VPN vers des passerelles VPN.

Visualiser le journal VPN

L'écran *Journal VPN* affiche le numéro de version du VPN Client.

Vous pouvez visualiser le type et le début du message, ainsi que son heure. Pour visualiser un message dans son ensemble, sélectionnez–le.

L'écran *Journal VPN* trie les messages par heure et par date en commençant par les plus récents. Vous pouvez visualiser les messages qui ont été enregistrés jusqu'à l'ouverture de l'écran *Journal VPN*. Appuyez sur *Options* et sélectionnez *Rafraîchir journal* pour afficher les messages les plus récents.

Les messages du journal peuvent contenir des codes d'erreur, d'état et de motif. Indiquez aux administrateurs les codes apparaissant dans les messages du journal, lorsque vous leur signalez des erreurs.

Effacer le journal VPN

Les messages du journal sont enregistrés dans une mémoire tampon circulaire. Ainsi, lorsque la taille du journal atteint 20 Ko, les nouveaux messages remplacent les plus anciens.

Pour effacer tous les messages du journal et vider l'écran *Journal VPN*, appuyez sur *Options* et sélectionnez *Effacer journal*.

7. Mots de passe d'enregistrement de clé

Un mot de passe d'enregistrement de clé permet de protéger les clés privées de l'appareil mobile et les connexions au serveur de politiques VPN contre toute utilisation non autorisée.

Allez à *Menu* et sélectionnez *Outils* > *Paramètres* > *Paramètres de connexion* > *Réseau privé virtuel (VPN)* > *Gestion VPN* > *Mot de passe enregistrement de clé*.

Créer ou modifier un mot de passe d'enregistrement de clé

Vous pouvez créer un mot de passe d'enregistrement de clé lors de l'installation de la première politique VPN. Si les pirates parviennent à deviner ou à déchiffrer un mot de passe d'enregistrement de clé, ils peuvent utiliser l'appareil mobile pour accéder au réseau d'entreprise protégé par le VPN. Vous devez donc créer des mots de passe d'enregistrement de clé suffisamment longs pour être difficiles à déchiffrer. Votre mot de passe doit rester secret. Ne l'inscrivez nulle part.

Pour créer ou modifier le mot de passe d'enregistrement de clé :

Dans *Nveau mot de passe d'enreg. de clés:*, saisissez un mot de passe facile à mémoriser pour vous et difficile à deviner pour toute autre personne.

Sélectionnez *Vérification du mot de passe:* et saisissez à nouveau le mot de passe pour éviter les erreurs de saisie.

Appuyez sur *OK* pour créer le mot de passe.

Astuce : Un mot de passe d'enregistrement de clé peut contenir des lettres et des chiffres et doit comporter au moins six caractères.

Saisir des mots de passe d'enregistrement de clé

Vous devez saisir le mot d'enregistrement de clé pour :

installer de nouvelles politiques VPN ou des politiques mises à jour depuis des serveurs de politiques VPN ;
utiliser des applications pour vous connecter à des points d'accès VPN nécessitant une authentification par certificat.

Remarque : Lorsque vous saisissez des mots de passe, l'écriture intuitive est désactivée. Entrez les caractères un par un. Par défaut, les lettres sont des minuscules.

8. VPN et applications

Lorsque vous utilisez une application pour créer une connexion VPN, VPN client :
se connecte au point d'accès Internet associé au point d'accès VPN ;
charge la politique VPN associée au point d'accès VPN ;
se connecte à une passerelle VPN pour créer une connexion VPN.

S'authentifier sur les passerelles VPN

Vous devez prouver votre identité lorsque vous vous connectez au réseau de votre entreprise. La politique VPN détermine la méthode d'authentification utilisée :

- Authentification par certificat : vous devez disposer d'un certificat signé par une autorité de certification fiable. Vous vous enregistrez en ligne pour obtenir le certificat requis ou vous installez les certificats lors de l'installation de la politique VPN depuis un fichier SIS.
- Authentification du type Legacy : vous utilisez des noms d'utilisateur et mots de passe ou codes pour vous authentifier. Les administrateurs créent les noms d'utilisateur et mots de passe requis ou vous fournissent les jetons SecurID nécessaires pour générer des codes d'authentification.

Si vous utilisez des certificats pour l'authentification, saisissez le mot de passe d'enregistrement de clé.

Si vous utilisez une authentification du type Legacy, saisissez les informations d'authentification VPN requises lorsque vous vous connectez à des points d'accès VPN à l'aide d'applications et que l'appareil mobile négocie des connexions cryptées avec la passerelle VPN.

Pour vous authentifier sur une passerelle VPN :

1. Saisissez votre nom d'utilisateur VPN dans *Nom d'utilisateur VPN:*.
2. Saisissez votre mot de passe ou code d'authentification VPN :
   - Saisissez votre mot de passe dans *Mot de passe VPN:*.

- Générez un code d'authentification SecurID, saisissez–le dans *Code d'authentification VPN:* et appuyez sur *OK*.

3 Si le jeton SecurID n'est plus synchronisé avec l'horloge de l'ACE/Server, vous êtes invité à saisir le prochain code d'authentification, que l'ACE/Server utilisera comme nouvelle référence temporelle du jeton.
Générez un code et saisissez–le dans *Prochain code d'authentification:*.
Si l'opération échoue, contactez les administrateurs.

4 Appuyez sur *OK*.

9. Dépannage

Le tableau suivant répertorie les messages d'erreur classés par ordre alphabétique, une description des causes possibles des erreurs, et des suggestions d'action corrective.

Message	Cause	Action
L'authentification a échoué. Vérifiez le nom d'utilisateur et le mot de passe.	• Le nom d'utilisateur ou le mot de passe que vous saisissez pour vous authentifier auprès d'un serveur de politiques VPN ou vous connecter à un VPN est incorrect. • Le code que vous saisissez lorsque vous êtes invité à entrer le prochain code n'est pas le bon.	• Vérifiez votre nom d'utilisateur et votre mot de passe et réessayez. • Attendez que le code d'authentification change, dans l'affichage du jeton SecurID, puis saisissez–le.

Message	Cause	Action
Mot de passe incorrect	Vous avez saisi un mot de passe d'enregistrement de clé ou d'importation de clé incorrect.	• Vérifiez le mot de passe et réessayez. • Les administrateurs vous fournissent le mot de passe d'importation de clé, mais c'est vous qui créez le mot de passe d'enregistrement de clé.
Code d'identification du serveur incorrect	La chaîne que vous saisissez lorsque vous êtes invité à entrer le code d'identification du serveur de politiques VPN est incorrecte.	Comparez attentivement le code d'identification du serveur de politiques VPN avec celui que vous ont fourni les administrateurs et saisissez à nouveau les caractères manquants.
Serveur de politiques actuellement utilisé. Impossible de le supprimer.	Vous ne pouvez pas supprimer un serveur de politiques VPN pendant que des politiques sont mises à jour depuis ce serveur. Lorsque vous utilisez une application pour créer une connexion VPN, les politiques VPN sont mises à jour automatiquement :	Attendez que la mise à jour soit terminée et réessayez.

Message	Cause	Action
Impossible d'activer une connexion VPN. Mettez d'abord à jour la politique VPN.	• Une authentification de type Legacy a échoué. • Le certificat que vous utilisez pour vous authentifier sur la passerelle VPN est manquant ou est arrivé à expiration, ou bien sa période de validité n'a pas encore commencé.	• Vérifiez votre nom d'utilisateur et votre mot de passe et réessayez. • Sélectionnez une politique dans l'écran *Politiques VPN*, appuyez sur *Options* et sélectionnez *Mise à jr politique* pour mettre à jour la politique. • Vérifiez les paramètres de date et d'heure sur l'appareil mobile.
Connexion impossible. Supprimez le serveur de politiques et redéfinissez les détails.	Le certificat du serveur de politiques VPN est parvenu à expiration.	Dans l'écran *Serveurs de politiques VPN* : 1 Appuyez sur *Options* et sélectionnez *Supprimer serveur* pour supprimer le serveur de politiques VPN. 2 Appuyez sur *Options* et sélectionnez *Nouveau serveur* pour ajouter à nouveau le serveur de politiques VPN, ou demandez à l'administrateur un fichier SIS contenant les nouveaux paramètres du serveur.

Message	Cause	Action
Connexion impossible. Entrez un nom d'utilis. et un mot de passe pour le serv. de politiques.	Le certificat qui vous authentifie sur le serveur de politiques VPN est arrivé à expiration ou les administrateurs ont révoqué le certificat.	• Signalez cette erreur aux administrateurs. Ils vous fourniront un mot de passe à usage unique pour vous connecter. • Saisissez le nom d'utilisateur et le mot de passe à usage unique pour vous authentifier sur le serveur de politiques VPN. • Un nouveau certificat est enregistré pour vous.
Connexion au serveur de politiques impossible. Consultez le journal VPN pour les détails.	La période de validité du certificat qui vous authentifie sur le serveur de politiques VPN n'a pas encore commencé.	Vérifiez les paramètres de date et d'heure ou attendez que la période de validité du certificat commence.

Message	Cause	Action
• *Impossible de mettre à jour la politique. Consultez le journal VPN pour les détails.* • *Synchronisation impossible. Consultez le journal VPN pour les détails.*	Une erreur s'est produite lors du téléchargement des politiques VPN depuis le serveur ou de leur installation sur l'appareil mobile.	• Dans l'écran *Politiques VPN*, sélectionnez une politique, appuyez sur *Options* et sélectionnez *Mise à jr politique* pour mettre à jour une politique VPN. • Dans l'écran *Serveurs de politiques VPN*, sélectionnez un serveur, appuyez sur *Options* et sélectionnez *Synchr. serveur* pour installer des politiques depuis ce serveur.
Politique VPN supprimée. Essayez de redéfinir le point d'accès VPN.	La politique VPN associée au point d'accès VPN a été supprimée car elle était obsolète.	Dans l'écran *Points d'accès VPN*, sélectionnez un point d'accès VPN, appuyez sur *Options* et sélectionnez *Edit* pour associer une autre politique VPN à ce point.

Index

A

Adresse du serveur de politiques, champ 15
Adresse serv. proxy, champ 18
aucun certificat 10
aucun point d'accès VPN 18
aucun serveur de politiques VPN 14
aucune politique VPN 9
authentification du type Legacy 23
authentification par certificat 23
avertissements de sécurité 14

C

certificats
- enregistrer 17
- état 10
- identifiant utilisateur 17
- s'authentifier sur les serveurs de politiques VPN 13

certificats expirés 10
certificats manquants 10
certificats pas encore valides 10
champs
- Adresse du serveur de politiques 15
- Adresse serv. proxy 18
- Code d'authentification VPN 24
- Description 9
- État de la politique 9, 10
- État du certificat 9
- Mis à jour 9
- Mot de passe serveur de politiques 16
- Mot de passe VPN 23
- N° port serv. proxy 18
- Nom d'utilisateur du serveur politiques 16
- Nom d'utilisateur VPN 23
- Nom de la connexion 18
- Nom de la politique 9
- Nom du serveur de politiques 15
- Nveau mot de passe d'enreg. de clés 21
- Point d'accès Internet 15, 18
- Politique VPN 18
- Prochain code d'authentification 24
- Serveur de politiques 9

client VPN
- configuration système requise 6
- utilisation 4

Code d'authentification SecurID 24
Code d'authentification VPN, champ 24
Code d'identification du serveur incorrect. 26
configuration mémoire requise 6
configuration système requise 6
Connexion au serveur de politiques impossible. Entrez un nom d'utilisateur et un mot de passe pour le serveur de politiques. 28
Connexion au serveur de politiques impossible. Pour plus de détails, voir le journal VPN. 28
Connexion au serveur de politiques impossible. Supprimez le serveur de politiques et redéfinissez les détails. 27

D

Description, champ 9

E

Effacer journal, option 20
enregistrement de clé 13
État de la politique, champ 9, 10
État du certificat, champ 9

I

Impossible d'activer la connexion VPN. Mettez d'abord à jour la politique VPN. 27
Impossible de mettre à jour la politique.

Pour plus de détails, voir le journal VPN. 29
installer
paramètres du serveur de politiques VPN depuis des fichiers SIS 13
installer des politiques VPN 16

J
Journal VPN
visualiser 20

L
L'authentification a échoué. Vérifiez le nom d'utilisateur et le mot de passe. 25

M
messages d'erreur 25
Mis à jour, champ 9
Modifier, option 18
Mot de passe incorrect. 26
Mot de passe serveur de politiques, champ 16
Mot de passe VPN, champ 23
mots de passe d'enregistrement de clé
à propos de 8, 21
création 21

N
N° port serv. proxy, champ 18
Nom d'utilisateur du serveur politiques, champ 16
Nom d'utilisateur VPN, champ 23
Nom de la connexion, champ 18
Nom de la politique, champ 9
Nom du serveur de politiques, champ 15
Nouv. point d'accès, option 18
Nouveau serveur, option 14
Nveau mot de passe d'enreg. de clés, champ 21

P
Point d'accès Internet, champ 15, 18
Points d'accès VPN
modifier 18
visualiser 18
points d'accès VPN
modifier 18
visualiser 19
Politique VPN supprimée. Essayez de redéfinir le point d'accès VPN. 29
Politique VPN, champ 18
Politiques VPN
état 10
mettre à jour 11
politiques VPN
suppression 12
visualisation 9
prochain code d'authentification 24
Prochain code d'authentification, champ 24

R
Rafraîchir, option 20

S
Serveur de politiques actuellement utilisé. Impossible de le supprimer. 26
Serveur de politiques, champ 9
Serveurs de politiques VPN
ajouter 14
installer les paramètres depuis des fichiers SIS 13
synchroniser 16
visualiser 14
serveurs de politiques VPN
connexion 13
Supprimer politique, option 12
Synchr. serveur, option 16
Synchronisation impossible. Pour plus de détails, voir le journal VPN. 29

U
Un 18

V
VPN 6
s'authentifier sur 23
utiliser avec des applications 23